

CLAIMS

What is claimed is:

- 1 1. A method of detecting a computer malware comprising the steps of:
 - 2 joining an Internet Relay Chat server;
 - 3 retrieving a list of channels of the Internet Relay Chat server;
 - 4 monitoring at least one channel in the list of retrieved channels;
 - 5 accepting data received from the monitored channel; and
 - 6 storing and logging the data received from the monitored channel.

- 1 2. The method of claim 1, wherein the monitoring step comprises the steps
2 of:
 - 3 joining a channel;
 - 4 waiting a time delay; and
 - 5 leaving the channel.

- 1 3. The method of claim 2, wherein the monitoring step further comprises the
2 step of:
 - 3 simulating user activities.

1 4. The method of claim 3, wherein the simulating step comprises the step of:
2 transmitting a message to the channel.

1 5. The method of claim 1, further comprising the step of:
2 scanning the received data to detect a computer malware.

1 6. The method of claim 5, wherein the computer malware comprises at least
2 one of a computer virus, a computer worm, or a computer Trojan horse program.

1 7. The method of claim 1, further comprising the step of:
2 analyzing the stored and logged data to detect a computer malware.

1 8. The method of claim 7, wherein the computer malware comprises at least
2 one of a computer virus, a computer worm, or a computer Trojan horse program.

1 9. The method of claim 7, further comprising the step of:
2 scanning the received data to detect a computer malware.

1 10. The method of claim 9, wherein the computer malware comprises at least
2 one of a computer virus, a computer worm, or a computer Trojan horse program.

1 11. The method of claim 7, wherein the monitoring step comprises the steps

2 of:

3 joining a channel;

4 waiting a time delay; and

5 leaving the channel.

1 12. The method of claim 11, wherein the monitoring step further comprises

2 the step of:

3 simulating user activities.

1 13. The method of claim 12, wherein the simulating step comprises the step

2 of:

3 transmitting a message to the channel.

1 14. The method of claim 13, wherein the computer malware comprises at

2 least one of a computer virus, a computer worm, or a computer Trojan horse

3 program.

1 15. A system for detecting a computer malware comprising:
2 a processor operable to execute computer program instructions;
3 a memory operable to store computer program instructions executable
4 by the processor; and
5 computer program instructions stored in the memory and executable to
6 perform the steps of:
7 joining an Internet Relay Chat server;
8 retrieving a list of channels of the Internet Relay Chat server;
9 monitoring at least one channel in the list of retrieved channels;
10 accepting data received from the monitored channel; and
11 storing and logging the data received from the monitored channel.

1 16. The system of claim 15, wherein the monitoring step comprises the steps
2 of:
3 joining a channel;
4 waiting a time delay; and
5 leaving the channel.

1 17. The system of claim 16, wherein the monitoring step further comprises the
2 step of:
3 simulating user activities.

1 18. The system of claim 17, wherein the simulating step comprises the step
2 of:
3 transmitting a message to the channel.

1 19. The system of claim 15, further comprising the step of:
2 scanning the received data to detect a computer malware.

1 20. The system of claim 19, wherein the computer malware comprises at least
2 one of a computer virus, a computer worm, or a computer Trojan horse program.

1 21. The system of claim 15, further comprising the step of:
2 analyzing the stored and logged data to detect a computer malware.

1 22. The system of claim 21, wherein the computer malware comprises at least
2 one of a computer virus, a computer worm, or a computer Trojan horse program.

1 23. The system of claim 21, further comprising the step of:
2 scanning the received data to detect a computer malware.

1 24. The system of claim 23, wherein the computer malware comprises at least
2 one of a computer virus, a computer worm, or a computer Trojan horse program.

1 25. The system of claim 21, wherein the monitoring step comprises the steps
2 of:
3 joining a channel;
4 waiting a time delay; and
5 leaving the channel.

1 26. The system of claim 25, wherein the monitoring step further comprises the
2 step of:
3 simulating user activities.

1 27. The system of claim 26, wherein the simulating step comprises the step
2 of:
3 transmitting a message to the channel.

1 28. The system of claim 27, wherein the computer malware comprises at least
2 one of a computer virus, a computer worm, or a computer Trojan horse program.

1 29. A computer program product for detecting a computer malware
2 comprising:

3 a computer readable medium;
4 computer program instructions, recorded on the computer readable
5 medium, executable by a processor, for performing the steps of
6 joining an Internet Relay Chat server;
7 retrieving a list of channels of the Internet Relay Chat server;
8 monitoring at least one channel in the list of retrieved channels;
9 accepting data received from the monitored channel; and
10 storing and logging the data received from the monitored channel.

1 30. The computer program product of claim 29, wherein the monitoring step
2 comprises the steps of:
3 joining a channel;
4 waiting a time delay; and
5 leaving the channel.

1 31. The computer program product of claim 30, wherein the monitoring step
2 further comprises the step of:
3 simulating user activities.

1 32. The computer program product of claim 31, wherein the simulating step
2 comprises the step of:
3 transmitting a message to the channel.

1 33. The computer program product of claim 29, further comprising the step
2 of:
3 scanning the received data to detect a computer malware.

1 34. The computer program product of claim 33, wherein the computer
2 malware comprises at least one of a computer virus, a computer worm, or a
3 computer Trojan horse program.

1 35. The computer program product of claim 29, further comprising the step
2 of:
3 analyzing the stored and logged data to detect a computer malware.

1 36. The computer program product of claim 35, wherein the computer
2 malware comprises at least one of a computer virus, a computer worm, or a
3 computer Trojan horse program.

1 37. The computer program product of claim 35, further comprising the step
2 of:
3 scanning the received data to detect a computer malware.

1 38. The computer program product of claim 37, wherein the computer
2 malware comprises at least one of a computer virus, a computer worm, or a
3 computer Trojan horse program.

1 39. The computer program product of claim 35, wherein the monitoring step
2 comprises the steps of:
3 joining a channel;
4 waiting a time delay; and
5 leaving the channel.

1 40. The computer program product of claim 39, wherein the monitoring step
2 further comprises the step of:
3 simulating user activities.

1 41. The computer program product of claim 40, wherein the simulating step
2 comprises the step of:
3 transmitting a message to the channel.

1 42. The computer program product of claim 41, wherein the computer
2 malware comprises at least one of a computer virus, a computer worm, or a
3 computer Trojan horse program.

1 43. A system for detecting computer malwares comprising:
2 a processor operable to execute computer program instructions;
3 a memory accessible by the processor, the memory comprising:
4 at least one Internet Relay Chat client operable to detect a
5 computer malware in an Internet Relay Chat channel; and
6 storage operable to store data received by the Internet Relay Chat
7 client.

1 44. The system of claim 43, wherein the Internet Relay Chat client is
2 operable to detect a computer malware by performing the steps of:
3 joining an Internet Relay Chat server;
4 retrieving a list of channels of the Internet Relay Chat server;
5 monitoring at least one channel in the list of retrieved channels;
6 accepting data received from the monitored channel; and
7 storing and logging the data received from the monitored channel in the
8 storage.

1 45. The system of claim 44, wherein the monitoring step comprises the steps
2 of:
3 joining a channel;
4 waiting a time delay; and
5 leaving the channel.

1 46. The system of claim 45, wherein the monitoring step further comprises the
2 step of:
3 simulating user activities.

1 47. The system of claim 46, wherein the simulating step comprises the step

2 of:

3 transmitting a message to the channel.

1 48. The system of claim 44, wherein the Internet Relay Chat client is further

2 operable to scan the received data to detect a computer malware.

1 49. The system of claim 48, wherein the computer malware comprises at least

2 one of a computer virus, a computer worm, or a computer Trojan horse program.

1 50. The system of claim 44, further comprising:

2 malware analysis software operable to analyze the stored and logged data

3 to detect a computer malware.

1 51. The system of claim 50, wherein the computer malware comprises at least

2 one of a computer virus, a computer worm, or a computer Trojan horse program.

1 52. The system of claim 50, wherein the Internet Relay Chat client is further

2 operable to scan the received data to detect a computer malware.

1 53. The system of claim 51, wherein the computer malware comprises at least
2 one of a computer virus, a computer worm, or a computer Trojan horse program.

1 54. The system of claim 50, wherein the monitoring step comprises the steps
2 of:

3 joining a channel;
4 waiting a time delay; and
5 leaving the channel.

1 55. The system of claim 54, wherein the monitoring step further comprises the
2 step of:

3 simulating user activities.

1 56. The system of claim 55, wherein the simulating step comprises the step
2 of:

3 transmitting a message to the channel.

1 57. The system of claim 56, wherein the computer malware comprises at least
2 one of a computer virus, a computer worm, or a computer Trojan horse program.